Fehlerbehebung für FirePOWER Data Path 4: Zugriffskontrollrichtlinie

Inhalt

[Einführung](#)
[Fehlerbehebung in der Phase "Access Control Policy (ACP)"](#)
[Auf Verbindungsvereignisse prüfen](#)
[Schnelle Schritte zur Minimierung](#)
[Debuggen des ACP](#)
[Beispiel 1: Datenverkehr stimmt mit einer Vertrauensregel überein](#)
[Beispiel 2: Datenverkehr, der einer Vertrauensregel entspricht, wird blockiert](#)
[Szenario 3: Blockierter Datenverkehr nach Anwendungs-Tag](#)
[Daten für TAC](#)
[Nächster Schritt: Fehlerbehebung auf der SSL-Richtlinienebene](#)

Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im Übersichtsartikel.

In diesem Artikel wird die vierte Phase der Fehlerbehebung für den FirePOWER-Datenpfad beschrieben: die Zugriffskontrollrichtlinie (Access Control Policy, ACP). Diese Informationen gelten für alle derzeit unterstützten Firepower-Plattformen und -Versionen.

Fehlerbehebung in der Phase "Access Control Policy (ACP)"

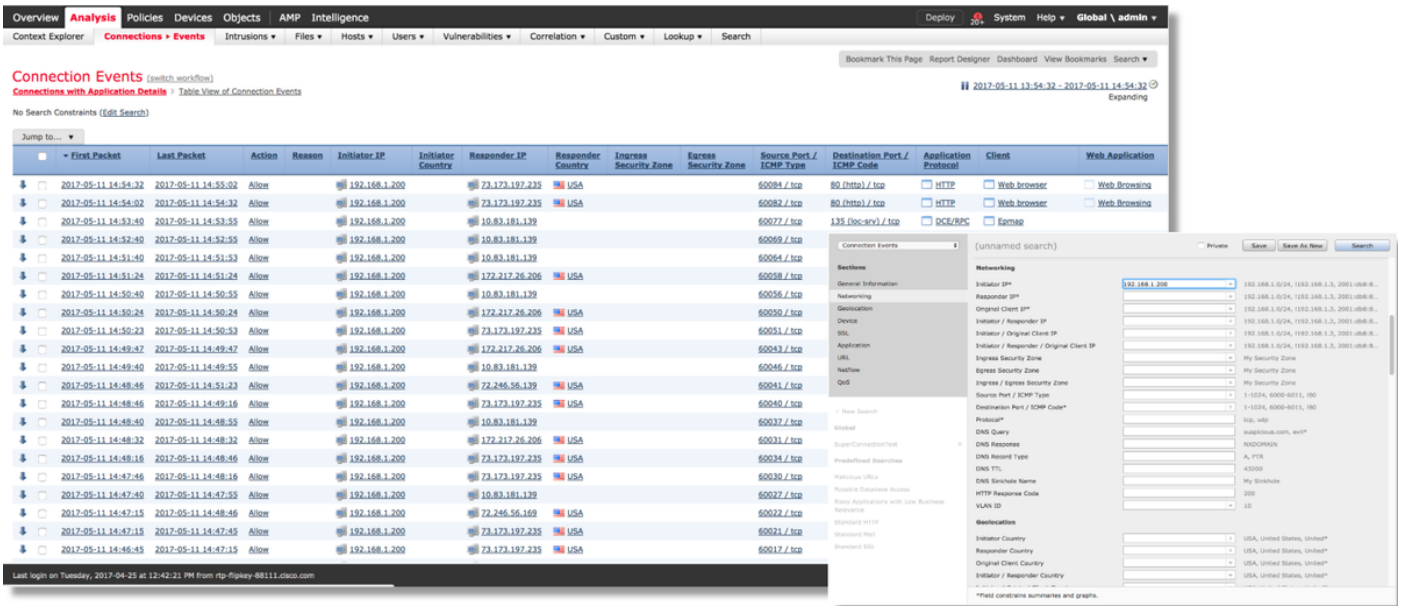
Im Allgemeinen sollte die Bestimmung, welche AKP-Regel ein Datenfluss gleicht, ziemlich geradlinig erfolgen. Die Verbindungsereignisse können überprüft werden, um festzustellen, welche Regel/Aktion erzwungen wird. Wenn dies nicht eindeutig anzeigt, was das ACP mit dem Datenverkehr tut, kann das Debuggen über die FirePOWER-Befehlszeilenschnittstelle (CLI) ausgeführt werden.

Auf Verbindungsvereignisse prüfen

Nachdem Sie eine Vorstellung von der Eingangs- und Ausgangsschnittstelle erhalten haben, sollten der Datenverkehr und die Datenflussinformationen übereinstimmen. Der erste Schritt zur Feststellung, ob FirePOWER den Datenfluss blockiert, besteht darin, die Verbindungsereignisse für den betreffenden Datenverkehr zu überprüfen. Diese können im FirePOWER Management

Center unter **Analysis > Connections > Events** angezeigt werden.

> **Hinweis**: Stellen Sie vor der Überprüfung von Connection Events sicher, dass die Protokollierung in Ihren ACP-Regeln aktiviert ist. Die Protokollierung wird in jeder Zugriffskontrollrichtlinie auf der Registerkarte "Protokollierung" sowie auf der Registerkarte "Sicherheitsinformationen" konfiguriert. Stellen Sie sicher, dass die fehlerverdächtigen Regeln so konfiguriert sind, dass sie die Protokolle an die Ereignisanzeige senden. Dies gilt auch für die Standardaktion.



Wenn Sie auf "Suche bearbeiten" klicken und von einer eindeutigen Quelle (Initiator)-IP gefiltert werden, können Sie die FirePOWER erkannten Flows sehen. In der Spalte Aktion wird für den Datenverkehr dieses Hosts "Zulassen" angezeigt.

Wenn FirePOWER Datenverkehr absichtlich blockiert, enthält die Aktion das Wort "Blockieren". Wenn Sie auf "Table View of Connection Events" (Tabellenansicht von Verbindungsereignissen) klicken, werden weitere Daten angezeigt. Die folgenden Felder in den Verbindungsereignissen können überprüft werden, wenn die Aktion "Blockieren" lautet:

- Grund

- Zugriffskontrollregel

Schnelle Schritte zur Minimierung

Um ein Problem, das vermutlich durch die AKP-Regeln verursacht wird, schnell zu beheben, kann Folgendes durchgeführt werden:

- Erstellen Sie eine Regel mit der Aktion "Trust" (Vertrauen) oder "Allow" (Erlauben) für den betreffenden Datenverkehr, und platzieren Sie diese an der Spitze der AKP-Regeln oder vor allem der Blockierungsregeln.
- Deaktivieren Sie vorübergehend alle Regeln mit einer Aktion, die das Wort "Block" enthält.
- Wenn die Standardaktion auf "Blockieren des gesamten Datenverkehrs" gesetzt ist, stellen Sie sie vorübergehend auf "Nur Netzwerkerkennung" um.

Hinweis: Diese schnellen Risikominderungen erfordern Richtlinienänderungen, die möglicherweise nicht in allen Umgebungen möglich sind. Es wird empfohlen, zunächst die Ablaufverfolgung der Systemunterstützung zu verwenden, um zu bestimmen, welche Regel der Datenverkehr erfüllt, bevor Richtlinienänderungen vorgenommen werden.

Debuggen des ACP

Weitere Fehlerbehebungen für die AKP-Vorgänge können mit der CLI-Utility **> Systemunterstützung für Firewall-Engine-Debugging** durchgeführt werden.

Hinweis: Auf den Firepower 9300- und 4100-Plattformen kann über die folgenden Befehle auf die betreffende Shell zugegriffen werden:

 # Connect-Modul 1-Konsole
Firepower-module1**> connect ftd**
>

Bei mehreren Instanzen kann mit den folgenden Befehlen auf die CLI des logischen Geräts zugegriffen werden.
 # Connect Module 1 Telnet
FirePOWER-module1**> connect ftd ftd1**
Herstellen einer Verbindung zur Containerkonsole ftd(ftd1) ... Geben Sie "exit" ein, um zur Boot CLI zurückzukehren.
>

Das **Firewall-Engine-Debug-**Dienstprogramm **für die Systemunterstützung** enthält einen Eintrag für jedes Paket, das vom ACP ausgewertet wird. Es zeigt den aktuellen Regelevaluierungsprozess sowie die Gründe, warum eine Regel zugeordnet oder nicht zugeordnet wird.

Hinweis: In Version 6.2 und höher kann das **Trace-**Tool zur **Systemunterstützung** ausgeführt werden. Sie verwendet dieselben Parameter, enthält jedoch weitere Details. Geben Sie bei Aufforderung "**Enable firewall-engine-debug ebenfalls aktivieren"** 'y **ein**.

Beispiel 1: Datenverkehr stimmt mit einer Vertrauensregel überein

Im folgenden Beispiel wird die Einrichtung einer SSH-Sitzung mithilfe von **systemunterstütztem Firewall-Engine-Debuggen** evaluiert.

Dies ist das ACP, das auf dem FirePOWER-Gerät ausgeführt wird.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

Die AKP-Staaten haben drei Regeln.

1. Die erste Regel gilt für Datenverkehr ab 192.168.0.7 mit von SSH verwendeten Zielports.
2. Die zweite Regel überprüft den gesamten von 10.0.0.0/8 eingehenden Datenverkehr, bei dem die Netzwerkkriterien auf der Grundlage der XFF-Headerdaten übereinstimmen (wie durch das Symbol neben dem Netzwerkobjekt angezeigt).
3. Die dritte Regel vertraut dem gesamten Datenverkehr zwischen 192.168.62.3 und 10.123.175.22.

Im Fehlerbehebungsszenario wird eine SSH-Verbindung zwischen 192.168.62.3 und 10.123.175.22 analysiert.

Es wird erwartet, dass die Sitzung mit der AC-Regel 3 "Trust Server Backup" übereinstimmt. Die Frage ist, wie viele Pakete benötigt werden, damit diese Sitzung mit dieser Regel übereinstimmt. Sind alle Informationen im ersten Paket erforderlich, um die Wechselstromregel oder mehrere Pakete zu bestimmen, und wenn ja, wie viele?

In der FirePOWER-CLI wird Folgendes eingegeben, um den Evaluierungsprozess für die AKP-Regel anzuzeigen.

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **Tipp**: Es ist am besten, möglichst viele Parameter auszufüllen, wenn **Firewall-Engine-Debuggen** ausgeführt wird, sodass nur die interessanten Debug-Meldungen auf dem Bildschirm ausgegeben werden.

In der Debug-Ausgabe unten sehen Sie die ersten vier Pakete der Sitzung, die ausgewertet werden.

SYN

SYN, ACK

ZURÜCK

Erstes SSH-Paket (Client an Server)

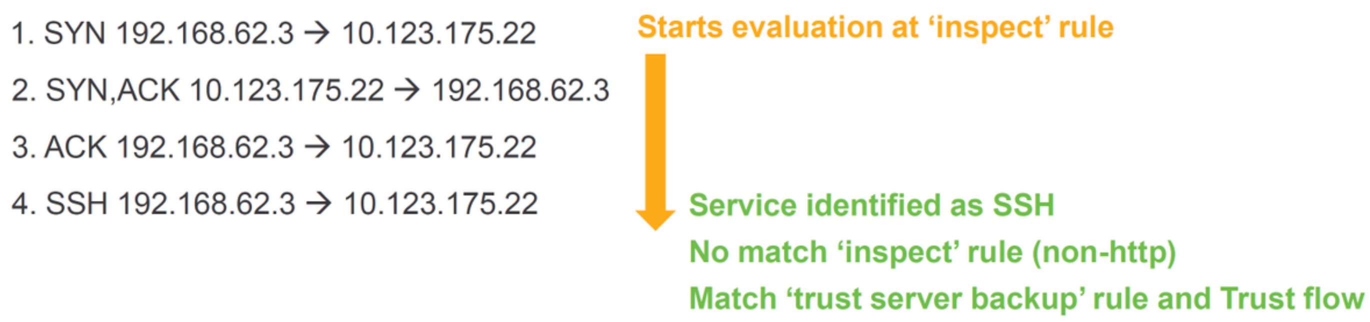
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Dies ist ein Diagramm, das die Debuglogik weiter veranschaulicht.



Für diesen Datenfluss sind vier Pakete erforderlich, damit das Gerät der Regel entspricht.

Dies ist eine detaillierte Erklärung der Debugausgabe.

- Der AKP-Evaluierungsprozess beginnt mit der Regel "inspect", da die Regel "trust ssh for host" nicht zugeordnet wurde, da die IP-Adresse nicht mit der Anforderung übereinstimmt. Dies ist eine schnelle Übereinstimmung, da alle Informationen erforderlich sind, um festzustellen, ob diese Regel im ersten Paket vorhanden ist (IPs und Ports).
- Es kann nicht bestimmt werden, ob der Datenverkehr mit der "inspect"-Regel übereinstimmt, bis die Anwendung identifiziert wurde, da X-Forwarded-For (XFF)-Informationen im HTTP-Anwendungsdatenverkehr gefunden werden. Da die Anwendung noch nicht bekannt ist, versetzt sie die Sitzung in einen ausstehenden Zustand für Regel 2, ausstehende Anwendungsdaten.
- Nachdem die Anwendung im vierten Paket identifiziert wurde, führt die "inspect"-Regel zu einer Nicht-Übereinstimmung, da die Anwendung SSH und nicht HTTP ist.
- Die Regel "trust server backup" wird dann auf Basis der IP-Adressen zugeordnet.

Zusammenfassend lässt sich feststellen, dass die Verbindung vier Pakete für die Sitzung benötigt, da sie auf die Firewall warten muss, um die Anwendung zu identifizieren, da Regel 2 eine Anwendungseinschränkung enthält.

Hätte Regel 2 nur Quellnetzwerke und nicht XFF gehabt, hätte dies ein Paket für die Sitzung benötigt.

Wenn möglich sollten Sie Layer-1-4-Regeln immer über alle anderen Regeln in der Richtlinie platzieren, da diese Regeln normalerweise ein Paket erfordern, um eine Entscheidung zu treffen. Sie können jedoch auch bemerken, dass selbst bei Layer-1-4-Regeln mehr als ein Paket einer AC-Regel entsprechen kann. Der Grund hierfür sind URL-/DNS-Sicherheitsinformationen. Wenn

Sie eine dieser Optionen aktivieren, muss die Firewall die Anwendung für alle Sitzungen festlegen, die von der AC-Richtlinie ausgewertet werden, da sie feststellen muss, ob es sich um HTTP oder DNS handelt. Anschließend muss er festlegen, ob die Sitzung auf der Grundlage der Blacklists zugelassen werden soll.

Unten sehen Sie eine gekürzte Ausgabe des Befehls **Firewall-Engine-Debugging**, bei dem die entsprechenden Felder rot hervorgehoben sind. Beachten Sie den Befehl, mit dem der Name der identifizierten Anwendung abgerufen wird.

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

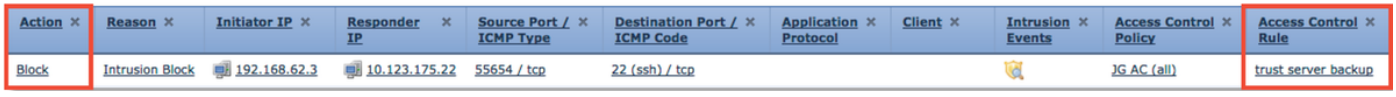
Beispiel 2: Datenverkehr, der einer Vertrauensregel entspricht, wird blockiert

In einigen Szenarien kann der Datenverkehr trotz Übereinstimmung mit einer Vertrauensregel in den AKP-Staaten blockiert werden. Im folgenden Beispiel wird Datenverkehr mit derselben Zugriffskontrollrichtlinie und denselben Hosts ausgewertet.

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```



Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Intrusion Events	Access Control Policy	Access Control Rule
Block	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp				JG AC (all)	trust server backup

Wie oben gezeigt, zeigt die **Firewall-Engine-Debugging**-Ausgabe, dass der Datenverkehr mit einem "Trust" übereinstimmt, während die Verbindungsereignisse Aktionen von **Block** aufgrund einer Intrusion Policy-Regel anzeigen (bestimmt, weil in der Spalte "Grund" der **Intrusion Block** angezeigt wird).

Dies kann auf die **Intrusion Policy** zurückzuführen sein**, die vor der Festlegung der Zugriffskontrollregel** auf der **Registerkarte Erweitert** auf dem ACP **verwendet wird**. Bevor der Datenverkehr anhand der Regelaktion als vertrauenswürdig eingestuft werden konnte, identifiziert die betreffende Richtlinie ein Muster-Übereinstimmung und verwirft den Datenverkehr. Die Evaluierung der AKP-Regeln führt jedoch zu einer Übereinstimmung mit der Vertrauensregel, da

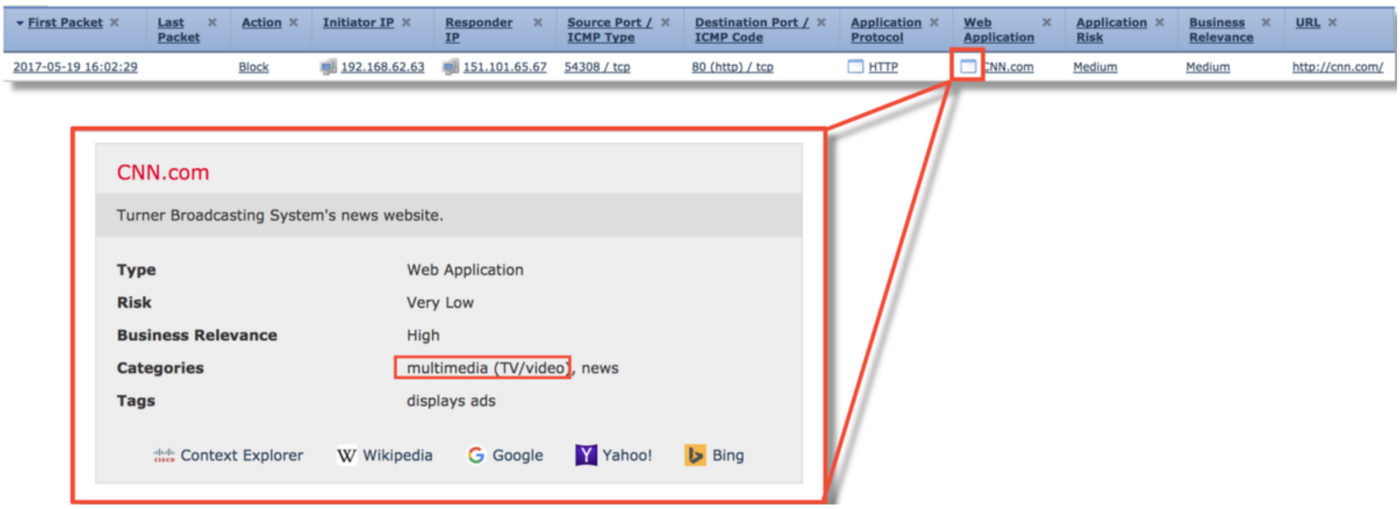
die IP-Adressen die Kriterien der "Vertrauensserver-Sicherung"-Regel erfüllten.

Damit der Datenverkehr nicht der Intrusion Policy Inspection (Prüfung der Richtlinie für Sicherheitsrisiken) unterzogen wird, kann die Vertrauensregel über der Regel "inspect" gesetzt werden. Dies ist in beiden Fällen eine Best Practice. Da die Anwendungsidentifizierung für eine Übereinstimmung und eine Nicht-Übereinstimmung der "inspect"-Regel erforderlich ist, wird die **Intrusion Policy, die vor der Festlegung der Zugriffskontrollregel verwendet wird,** für Datenverkehr verwendet, der von derselben Regel ausgewertet wird. Wenn die Regel für die "Vertrauensserver-Sicherung" oberhalb der Regel "inspect" platziert wird, stimmt der Datenverkehr mit der Regel überein, wenn das erste Paket angezeigt wird, da die Regel auf der IP-Adresse basiert, die im ersten Paket festgelegt werden kann. Daher muss die **Intrusion Policy, die vor der Festlegung der Zugriffskontrollregel verwendet wird,** nicht verwendet werden.

Szenario 3: Blockierter Datenverkehr nach Anwendungs-Tag

In diesem Szenario melden Benutzer, dass cnn.com blockiert wird. Es gibt jedoch keine bestimmte Regel, die CNN blockiert. Die Connection-Ereignisse in Verbindung mit der Ausgabe von **Firewall-Engine-Debugging** zeigen den Grund für den Block.

Zuerst enthält das Feld Connection Events (Verbindungsereignisse) neben den Anwendungsfeldern ein Informationsfeld, das Informationen über die Anwendung sowie die Kategorisierung der Anwendung durch FirePOWER anzeigt.

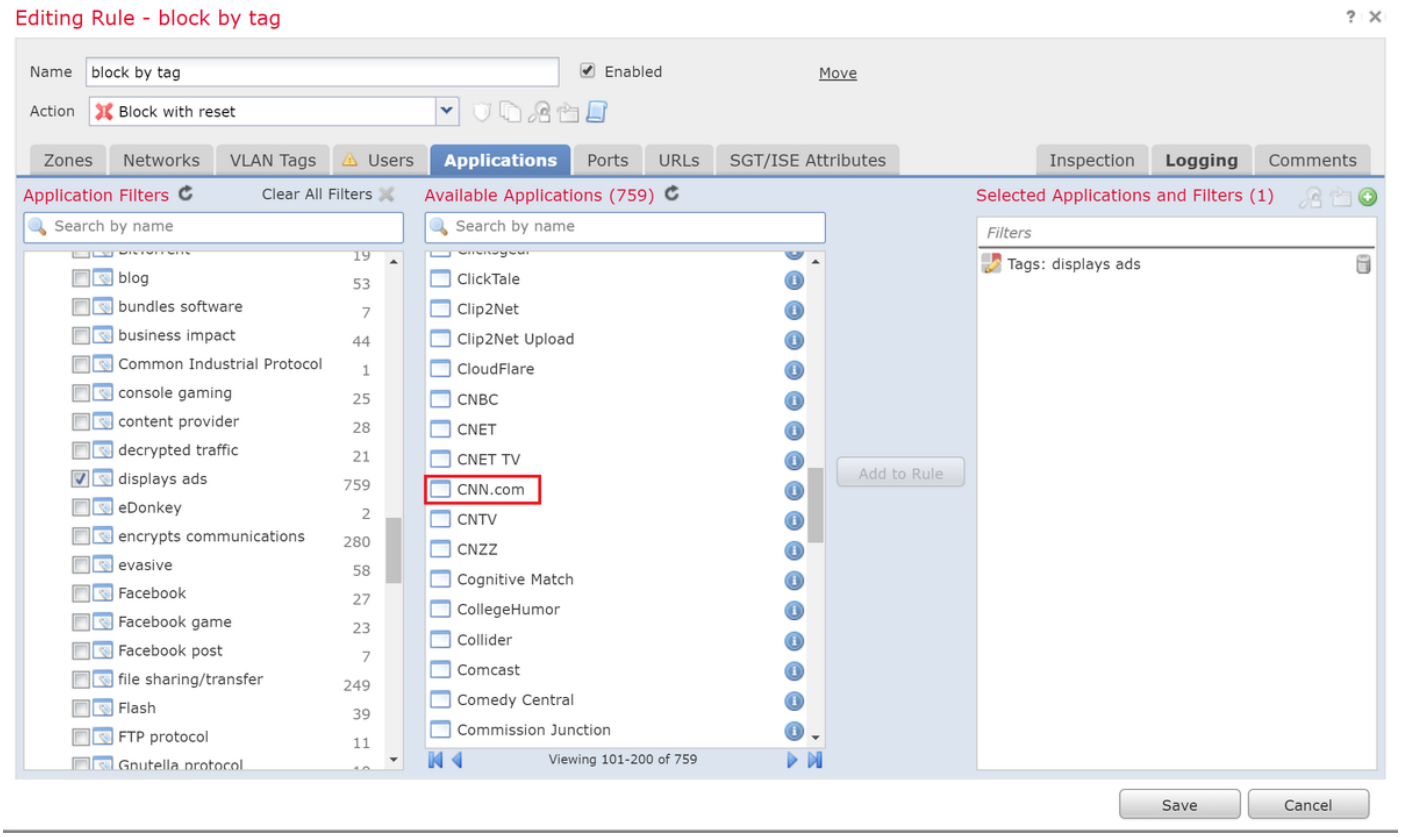


Unter Berücksichtigung dieser Informationen wird **Firewall-Engine-Debugging** ausgeführt. In der Debugausgabe wird der Datenverkehr basierend auf dem Anwendungstag blockiert.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

Obwohl es keine Regel gibt, die explizit http://cnn.com blockiert, werden **Anzeigen** mit Tags auf

der Registerkarte **Anwendungen** einer AKP-Regel blockiert.



Daten für TAC

Daten	Anweisungen
Fehlerbehebungsdatei vom FirePOWER-Gerät, die den Datenverkehr prüft	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1
Systemunterstützung Firewall-Engine-Debug und **System-Support-Trace**-Ausgabe	Anweisungen hierzu finden Sie in diesem Artikel
Export von Zugriffskontrollrichtlinien	Navigieren Sie zu **System > Extras > Importieren/Exportieren**, wählen Sie die Zu klicken Sie auf die Schaltfläche **Exportieren**

> **Vorsicht**: Wenn das ACP eine SSL-Richtlinie enthält, entfernen Sie die SSL-Richtlinie aus dem ACP, bevor Sie exportieren, um die Offenlegung vertraulicher PKI-Informationen zu vermeiden.

Nächster Schritt: Fehlerbehebung auf der SSL-Richtlinienebene

Wenn eine SSL-Richtlinie verwendet wird und das Problem bei der Fehlerbehebung für die Zugriffskontrollrichtlinie nicht erkannt wurde, besteht der nächste Schritt darin, eine Fehlerbehebung für die SSL-Richtlinie durchzuführen.

Klicken Sie hier, um mit dem nächsten Artikel fortzufahren.